文章编号:1005-3085(2010)03-0521-06

环 Z_{pq} 上逻辑函数的分解及其应用*

赵亚群， 金栋梁

(信息工程大学信息工程学院，郑州 450002)

摘 要: 为克服一般剩余类环上合数值逻辑函数无统一多项式表示给函数研究工作带来的困难，本文利用中国剩余定理对环 Z_{pq} ($p<q$ 且均为素数) 上的 pq 值随机变量进行了分解；并由此对 pq 值逻辑函数及其变元进行了CRT-分解，给出了 pq 值逻辑函数的分解函数的代数标准型，据此可得 pq 值逻辑函数在CRT-分解意义下的代数标准型；又讨论了 pq 值相关免疫逻辑函数在CRT-分解意义下的等价判别条件，给出了利用分解函数的代数标准型构造 pq 值相关免疫逻辑函数的一种方法。

关键词: pq 值逻辑函数；CRT-分解；代数标准型；相关免疫；分解谱

分类号: **AMS**(2000) 94C10; 06E30 **中图分类号**: TN918.1 **文献标识码**: A

1 引言和基本概念

由于实际应用的需要，近年来人们对密码学中的多值逻辑函数给予了较多的关注。由文献 [1] 可知，素域 Z_p (p 为素数) 上的多值逻辑函数如同布尔函数一样也具有代数表示形式 (称为多项式表示)，且布尔函数的很多结论[2-4] 和研究方法可以直接推广到素域上。但对于一般的合数 m，由于环与素域的差异，给研究合数值逻辑函数的性质及构造等工作带来了较大的困难。文献 [5] 给出了 4 值 n 元逻辑函数在 2-基分解意义下转化为具有某类特殊性质相互关系的两个 $2n$ 元布尔函数。文献 [6] 给出了 p^l ($l>1$) 值逻辑函数的代数标准型，文献 [7] 研究了 p^l 值逻辑函数与其 p-基分解意义下向量函数之间的关系。文献 [8] 分析了 p^l 值相关免疫逻辑函数的代数结构。文献 [9] 也在 p-基分解意义下对 p^l 值相关免疫逻辑函数进行了分解，将环上相关免疫逻辑函数的判定问题转化为素域上向量逻辑函数满足适定条件问题。对于环 Z_{pq} 是否有类似的结论?

本文首次利用中国剩余定理对环 Z_{pq} 上的 pq 值随机变量进行分解，得到了 pq 值逻辑函数在CRT-分解意义下的代数标准型，给出了利用分解函数的代数标准型构造 pq 值相关免疫逻辑函数的一种方法。结合 p-基分解和CRT-分解这两种代数分析方法，我们可以给出环上任意逻辑函数的代数表示形式，为研究具有特殊密码学性质的多值逻辑函数的构造方法提供了新的理论依据和有效工具。

设 $m\geq 2$ 是任一取定的正整数，$Z_m=Z/(m)$ 为整数模 m 的剩余类环。又设 n 为任一正整数，$X=(X_1,\cdots,X_n)$ 中的 $X_1,\cdots,X_n$ 都是定义在某概率空间上相互独立、且都具有均匀分布的 m 值随机变量，记 m 次本原单位根为 $u_m=\mathrm{e}^{2\pi i/m}$，$i=\sqrt{-1}$。称 $Z_m^n\to Z_m$ 的任一映射 $f(x)$, $x\in Z_m^n$ 为 Z_m^n 上的 n 元 m 值逻辑函数。对任意的 $a\in Z_m^n$，$I_{\{a\}}(x)$, $x\in Z_m^n$ 为 a 的示性函数，$W_H(a)$ 为 a 的Hamming重量。逻辑函数的Chrestenson循环谱和相关免疫相关免疫性见文献 [2-4]。下文总设 p,q 为素数，且不妨设 $p<q$。

收稿日期: 2008-04-28. **作者简介**: 赵亚群 (1961年4月生)，女，教授. 研究方向：密码基础理论及概率统计应用.
***基金项目**: 信息安全国家重点实验室开放基金 (01-02).

2　pq 值逻辑函数的分解

定理 1 (中国剩余定理 (CRT))[10]　设 $m_1,\cdots,m_r$ 是 r 个两两互素的正整数，令 $m=m_1,\cdots,m_r$，$m=m_iM_i$，$M_i'M_i\equiv 1\,(\mathrm{mod}m_i)$，$1\le i\le r$，则一次同余方程组

$$x\equiv x_1\,(\mathrm{mod}m_1),\cdots,x\equiv x_r\,(\mathrm{mod}m_r),\tag{1}$$

有惟一解

$$x\equiv M_1'M_1x_1+M_2'M_2x_2+\cdots+M_r'M_rx_r\,(\mathrm{mod}m).\tag{2}$$

命题 1　设 (Ω,F,P) 是某一概率空间，Z 是 Ω 到 Z_{pq} 的映射，则：

1)　Z 可以由中国剩余定理分解为

$$Z(\omega)=M_1'M_1X(\omega)+M_2'M_2Y(\omega),\tag{3}$$

其中

$$M_1=q,\quad M_2=p,\quad M_1'M_1\equiv 1\,(\mathrm{mod}p),\quad M_2'M_2\equiv 1\,(\mathrm{mod}q),$$

$$X(\omega)\in Z_p,\quad Y(\omega)\in Z_q,\quad \omega\in\Omega.$$

2)　Z 是概率空间 (Ω,F,P) 上 pq 值随机变量的充要条件是 X,Y 都是 (Ω,F,P) 上的随机变量。

证明　由中国剩余定理和随机变量相互独立的定义易得。

性质 1　设 Z 是某概率空间 (Ω,F,P) 上的 pq 值随机变量，则 Z 具有“均匀分布”的充分必要条件是 X,Y 相互独立，且都具有“均匀分布”，其中 Z,X,Y 满足 (3) 式。

文献 [1] 指出：当 m 是素数时，任一 m 值逻辑函数可以由模 m 多项式表示，而当 m 是合数时，并不是所有 m 值逻辑函数都能用模 m 多项式表示。文献 [11] 只给出了多值逻辑函数具有多项式表示的条件，下面给出所有 pq 值逻辑函数 (无论有无多项式表示) 的一种统一分解表示式。

根据中国剩余定理，在 Z_{pq} 和 $Z_p\times Z_q$ 之间建立如下一一对应关系

$$z\in Z_{pq}\Leftrightarrow(x,y)\in Z_p\times Z_q,$$

其中

$$z\equiv M_1'M_1x+M_2'M_2y\,(\mathrm{mod}pq),\quad M_1=q,\quad M_2=p,$$

$$M_1'M_1\equiv 1\,(\mathrm{mod}p),\quad M_2'M_2\equiv 1\,(\mathrm{mod}q).$$

记 $z=(z_1,\cdots,z_n)\in Z_{pq}^n$ 对应的分解分量为

$$x=(x_1,\cdots,x_n)\in Z_p^n,\quad y=(y_1,\cdots,y_n)\in Z_q^n.$$

设 $f(z)$，$z\in Z_{pq}^n$ 是任意的 n 元 pq 值逻辑函数，则在上述建立的一一对应分解意义下有

$$f(z)=M_1'M_1f_1(x;y)+M_2'M_2f_2(x;y),\tag{4}$$

其中 $(x;y)\in Z_p^n\times Z_q^n$，$f_1(x;y)$ 是 $Z_p^n\times Z_q^n$ 到 Z_p 的映射，而 $f_2(x;y)$ 是 $Z_p^n\times Z_q^n$ 到 Z_q 的映射。我们把上述逻辑函数的分解称为 **CRT-**分解。称 $f_1(x;y)$，$f_2(x;y)$，$(x;y)\in Z_p^n\times Z_q^n$ 为 $f(z)$ 的 CRT-分解意义下的分解函数，简称分解函数，简记为 $[f_1,f_2]$。

3 pq 值逻辑函数的代数标准型

首先，在CRT-分解意义下，寻求分解函数 $[f_1, f_2]$ 的代数标准型。

引理 1[10] 对任意正整数 m 及 $a, r \in Z_m\backslash\{0\}$，$\gcd(a, m) = 1$，同余方程

$$ax \equiv r\,(\mathrm{mod} m) \tag{5}$$

在 Z_m 中有惟一解。

定理 2 设 $f_1(x;y)$, $(x;y) \in Z_p^n \times Z_q^n$，是 $Z_p^n \times Z_q^n$ 到 Z_p 上的映射，则 $f_1(x;y)$ 具有如下表示

$$f_1(x;y) = \sum_{i_1,\cdots,i_n \in Z_p} \Big\{a_{i_1,\cdots,i_n} x_1^{i_1}, \cdots, x_n^{i_n}(\mathrm{mod} p) \times \Big[\sum_{j_1,\cdots,j_n \in Z_q} b_{j_1,\cdots,j_n} y_1^{j_1}, \cdots, y_n^{j_n}(\mathrm{mod} q)\Big]\Big\}, \tag{6}$$

其中 $a_{i_1,\cdots,i_n}$，$i_1,\cdots,i_n \in Z_p$，$b_{j_1,\cdots,j_n}$，$j_1,\cdots,j_n \in Z_q$，且在上述定义运算下表法是惟一的。

证明 首先注意到，对任意的映射可有如下表示：对任意的 $(x;y) \in Z_p^n \times Z_q^n$，有

$$f_1(x;y) = \sum_{(a;b)\in Z_p^n \times Z_q^n} f_1(a;b) I_{\{(a;b)\}}(x;y) = \sum_{\substack{a=(a_1,\cdots,a_n)\in Z_p^n \\ b=(b_1,\cdots,b_n)\in Z_q^n}} f_1(a;b) \prod_{i=1}^{n} I_{\{a_i\}}(x_i) I_{\{b_i\}}(y_i), \tag{7}$$

其中 $\sum$ 为剩余类环 Z_p 上的运算，$I_{\{(a;b)\}}(x;y)$，$I_{\{a_i\}}(x_i)$，$I_{\{b_i\}}(y_i)$ 均为示性函数。

$I_{\{a_i\}}(x_i)$ 是 Z_p 上的逻辑函数，由有限域知识[1] 可知 $I_{\{a_i\}}(x_i)$ 存在惟一的多项式表示，可设

$$I_{\{a_i\}}(x_i) \equiv c\big(x_i + (p-1)a_i + 1\big)\big(x_i + (p-1)a_i + 2\big) \cdots \big(x_i + (p-1)a_i + p - 1\big)(\mathrm{mod} p), \tag{8}$$

其中 $c \in Z_p$ 满足：$c \cdot 1 \cdot 2 \cdots (p-1) \equiv 1\ (\mathrm{mod} p)$，由引理 1 可知 c 有惟一解。而 $I_{\{b_i\}}(y_i)$ 是 Z_q 到 Z_p 上的映射，将 Z_q 上的 0 和 1 映射到 Z_p 上的 0 和 1，则有

$$I_{\{b_i\}}(y_i) \equiv d(y_i + (q-1)b_i + 1)(y_i + (q-1)b_i + 2) \cdots (y_i + (q-1)b_i + q - 1)\ (\mathrm{mod} q), \tag{9}$$

其中 $d \in Z_q$ 满足

$$d \cdot 1 \cdot 2 \cdots (q-1) \equiv 1\ (\mathrm{mod} q),$$

而

$$\gcd\big(1 \cdot 2 \cdots (q-1), q\big) = 1,$$

由引理 1 可知 d 有惟一解，此时是将 Z_q 上的 0 和 1 映射到 Z_p 上的 0 和 1，且在此意义下表法惟一。

根据 (7), (8), (9) 式，我们有

$$f_1(x;y) = \sum_{\substack{a=(a_1,\cdots,a_n)\in Z_p^n \\ b=(b_1,\cdots,b_n)\in Z_q^n}} f_1(a;b) \Big[\prod_{i=1}^{n} c \prod_{j\in Z_p\backslash\{0\}} (x_i + (p-1)a_i + j)\ (\mathrm{mod} p)\Big] \times \Big[\prod_{i=1}^{n} d \prod_{j\in Z_q\backslash\{0\}} (y_i + (q-1)b_i + j)(\mathrm{mod} q)\Big]. \tag{10}$$

因为 $f_1(x;y)$ 与 $f_1(a;b)$ 相互惟一确定，故 (10) 式在定义运算下表法惟一。将 (10) 式两个中括号内的各乘积项展开、合并并化简即可得 (6) 式，即结论得证。

定理3 设 $f_2(x;y)$, $(x;y)\in Z_p^n\times Z_q^n$ 是 $Z_p^n\times Z_q^n$ 到 Z_q 上的映射，则 $f_2(x;y)$ 具有如下表示

$$f_2(x;y)=\sum_{i_1,\cdots,i_n\in Z_p}\sum_{j_1,\cdots,j_n\in Z_q} d_{i_1,\cdots,i_n;j_1,\cdots,j_n}x_1^{i_1}\cdots x_n^{i_n}y_1^{j_1}\cdots y_n^{j_n}\ (\mathrm{mod}q), \tag{11}$$

其中 $d_{i_1,\cdots,i_n;j_1,\cdots,j_n}\in Z_q$，$i_1,\cdots,i_n\in Z_p$，$j_1,\cdots,j_n\in Z_q$，且在上述表法是惟一的。

证明 同定理2一样，首先注意到对任意的映射可有如下表示

$$f_2(x;y)=\sum_{\substack{a=(a_1,\cdots,a_n)\in Z_p^n\\ b=(b_1,\cdots,b_n)\in Z_q^n}} f_2(a;b)\prod_{i=1}^n I_{\{a_i\}}(x_i)I_{\{b_i\}}(y_i),\quad (x;y)\in Z_p^n\times Z_q^n, \tag{12}$$

$I_{\{b_i\}}(y_i)$ 是 Z_q 上的逻辑函数，同定理2证明一样可有惟一多项式表示。而 $I_{\{a_i\}}(x_i)$ 是 Z_p 到 Z_q 上的映射，将 Z_p 中元素视为 Z_q 上的元素，则分下面两种情况讨论。

(I) $p=2$ 时：

当 $a_i=0$ 时，记

$$I_{\{a_i\}}(x_i)\equiv d_0(x_i-1)\ (\mathrm{mod}q), \tag{13}$$

其中 $d_0\in Z_q$ 满足方程：$(-1)d_0\equiv 1\ (\mathrm{mod}q)$。由引理1可知 d_0 有惟一解，即 (13) 式为 $I_{\{a_i\}}(x_i)$ 的惟一多项式表示。

当 $a_i=1$ 时，记

$$I_{\{a_i\}}(x_i)\equiv x_i\ (\mathrm{mod}q). \tag{14}$$

(II) p 为奇素数时：

当 $a_i=0$ 时，记

$$I_{\{a_i\}}(x_i)\equiv d_0(x_i-1)\cdots(x_i-(p-1))\ (\mathrm{mod}q), \tag{15}$$

其中 $d_0\in Z_q$ 满足方程

$$d_0\cdot 1\cdot 2\cdots(p-1)\equiv 1\ (\mathrm{mod}q).$$

而

$$\gcd\big(1\cdot 2\cdots(p-1),q\big)=1,$$

由引理1可知 d_0 有惟一解，即 (15) 式为 $I_{\{a_i\}}(x_i)$ 的惟一多项式表示，且表法惟一。

当 $a_i=1$ 时，记

$$I_{\{a_i\}}(x_i)\equiv d_1x_i(x_i-2)\cdots(x_i-(p-1))\ (\mathrm{mod}q). \tag{16}$$

当 $a_i=p-1$ 时，记

$$I_{\{a_i\}}(x_i)\equiv d_{p-1}x_i(x_i-1)(x_i-2)\cdots(x_i-(p-2))\ (\mathrm{mod}q). \tag{17}$$

当 $a_i\in Z_p\backslash\{0,1,p-1\}$ 时，记

$$I_{\{a_i\}}(x_i)\equiv d_{a_i}x_i(x_i-1)\cdots(x_i-a_i+1)(x_i-a_i-1)\cdots(x_i-(p-1))\ (\mathrm{mod}q), \tag{18}$$

其中 $d_i \in Z_q$，$i=0,1,\cdots,p-1$，且满足

$$d_1 \cdot 1 \cdot (-1) \cdots (2-p) \equiv 1\ (\mathrm{mod} q),$$

$$d_{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 1\ (\mathrm{mod} q),$$

$$d_{a_i} \cdot 1 \cdots a_i \cdot (-1) \cdots (a_i - p + 1) \equiv 1\ (\mathrm{mod} q).$$

注意到 $p<q$，同样由引理1可知，d_i，$i=0,1,\cdots,p-1$ 具有惟一解，因此式(16),(17),(18)表法惟一。与定理2证明一样，进行展开、合并并化简，即知结论成立。

由定理2、3及CRT—分解可见，pq 值逻辑函数在定义的运算下具有惟一的代数标准型。

4　pq 值相关免疫逻辑函数的等价判别条件

定义1　设 $f(z)$, $z \in Z_{pq}^n$ 是 n 元 pq 值逻辑函数，$[f_1,\ f_2]$ 是 $f(z)$ 的相应分解函数。称

$$S_{(f_1,f_2)}(w^{(1)};w^{(2)}) = \frac{1}{(pq)^n} \sum_{x\in Z_p^n} \sum_{y \in Z_q^n} u_p^{f_1(x;y)-w^{(1)}\cdot x} u_q^{f_2(x;y)-w^{(2)}\cdot y}, \quad (w^{(1)};w^{(2)}) \in Z_p^n \times Z_q^n \tag{19}$$

为逻辑函数 $f(z)$ 的 Chrestenson 循环分解谱，简称为 $f(z)$ 的分解谱。

定义2　称 $(w_{11};w_{12}) \in Z_p \times Z_q, \cdots, (w_{n1};w_{n2}) \in Z_p \times Z_q$ 为向量 $w=(w_{11},\cdots,w_{n1};w_{12},\cdots,w_{n2}) \in Z_p^n \times Z_q^n$ 的正规分划，记

$$W_j(w_{j1};w_{j2}) = \begin{cases} 1, & (w_{j1};w_{j2}) \neq 0, \\ 0, & (w_{j1};w_{j2}) = 0, \end{cases} \qquad 0 \in Z_p \times Z_q, \quad 1 \le j \le n,$$

称 $\overline{W}(w) = \sum_{j=1}^{n} W_j(w_{j1};w_{j2})$ 为 w 的正规分划汉明重量。

引理2[3,4]　m 值逻辑函数 $f(z_1,\cdots,z_n)$, $(z_1,\cdots,z_n) \in Z_m^n$ 为 t 阶相关免疫的充分必要条件是对任意的 $w \in Z_m^n$，其汉明重量 $1 \le W_H(w) \le t$ 时，都有

$$S_{(\lambda f)}(w) = 0, \quad \lambda \in Z_m \backslash \{0\}. \tag{20}$$

定理4　设 $f(z)$, $z \in Z_{pq}^n$ 是 n 元 pq 值逻辑函数，$[f_1, f_2]$ 是 $f(z)$ 的相应分解函数，则 $f(z)$ 是 t 阶相关免疫的充分必要条件是对任意的 $w=(w^{(1)};w^{(2)}) \in Z_p^n \times Z_q^n$，及 $1 \le \overline{W}(w) \le t$，$\lambda_1 \in Z_p$，$\lambda_2 \in Z_q$ 且 λ_1、λ_2 不同时为零时，都有 $f(z)$ 的分解谱满足

$$S_{(\lambda_1 f_1, \lambda_2 f_2)}\big(w^{(1)};w^{(2)}\big) = 0. \tag{21}$$

证明　由引理2可知，$f(z)$ 是 t 阶相关免疫的充分必要条件是对任意的 $\lambda \in Z_{pq}\backslash\{0\}$ 及任意的 $v \in Z_{pq}^n$，其汉明重量 $1 \le W_H(v) \le t$ 时，都有 $S_{(\lambda f)}(v) = 0$。由定理1，对 $f(z)$, $z \in Z_{pq}^n$，$v \in Z_{pq}^n$ 及 $\lambda \in Z_{pq}$ 进行CRT—分解有 $S_{(\lambda f)}(v) = S_{(M_1'\lambda_1 f_1, M_2'\lambda_2 f_2)}(w^{(1)};w^{(2)})$，其中 v 的分解分量为 $(w^{(1)};w^{(2)})$。由引理2、中国剩余定理分解的惟一性可知结论成立。

参考文献：

[1] Lidl R, Niederreiter H. Finite Field[M]. London: Addison-wesley Publishing Company, 1984

[2] 丁存生，肖国镇. 流密码学及其应用[M]. 北京：国防工业出版社，1994
Ding C S, Xiao G Z. Stream Cipher and its Application[M]. Beijing: National Defence Industry Press, 1994

[3] 冯登国. 频谱理论及其在密码学中应用[M]. 北京：科学出版社，2000
Feng D G. The Application of Spectral Theory in Cryptology[M]. Beijing: Science Press, 2000

[4] 李世取，曾本胜，廉玉忠等. 密码学中的逻辑函数[M]. 北京：中软电子出版社，2003
Li S Q, Zeng B S, Lian Y Z, *et al.* Logical Functions in Cryptology[M]. Beijing: China National Computer Software and Technology Service Corporation Press, 2003

[5] 张文英，李世取，孙旭. Z_4^n 上完全非线性函数的存在性和构造[J]. 工程数学学报，2004, 21(2): 149-154
Zhang W Y, Li S Q, Sun X. The existence and construction of perfect nonlinear functions on Z_4^n[J]. Chinese Journal of Engineering Mathematics, 2004, 21(2): 149-154

[6] 王隽，李世取，刘文芬. m 值逻辑函数的代数标准型[J]. 通信保密，1999, (2): 28-34
Wang J, Li S Q, Liu W F. Algebraic of m-valued logical functions[J]. Communication and Secrecy, 1999, (2): 28-34

[7] 王隽，陈卫红. 环 Z_{p^l} 上的逻辑函数[J]. 通信保密，2000, (2): 41-44
Wang J, Chen W H. Logical functions over ring Z_{p^l}[J]. Communication and Secrecy, 2000, (2): 41-44

[8] 刘文芬，李世取. 环 Z_{p^l} 上平衡相关免疫多值逻辑函数的代数结构分析[J]. 高校应用数学学报 A 辑，2001, 16(1): 1-7
Liu W F, Li S Q. Algebraic structure analyses of balanced correlation immunity multiple-valued logical functions over ring Z_{p^l}[J]. Applied Mathematics: A Journal of Chinese University, 2001, 16(1): 1-7

[9] 杨锐，曾本胜，李世取. p^r 值逻辑函数相关免疫的等价判别条件[J]. 应用数学，2006, 19(1): 139-144
Yang R, Zeng B S, Li S Q. Criterion of correlation immunity for p^r-value logical functions[J]. Applied Mathematics, 2006, 19(1): 139-144

[10] 柯召，孙琦. 数论讲义[M]. 北京：高等教育出版社，1987
Ke Z, Sun Q. An Introduction to Number Theory[M]. Beijing: Higher Education Press, 1987

[11] Meshchaninov D G. A method for constructing polynomials of k-valued logic functions[J]. Discrete Math Appl, 1995, 5(4): 333-346

Decomposition of Logical Functions over Ring Z_{pq} and its Application

ZHAO Ya-qun, JIN Dong-liang

(Information Engineering Institute, Information Engineering University, Zhengzhou 450002)

Abstract: To overcome the difficulty that the composite-valued logical functions over the residual class ring can not be represented by canonical polynomials, the decompositions for pq-valued random variables are presented by the Chinese remainder theorem (CRT), and the CRT-decompositions of the pq-valued logical functions and their variables are shown, and the algebraic normal form of decomposable functions for pq-valued logical functions is obtained. The algebraic normal form for pq-valued logical functions is presented under the according CRT-decomposition. Then the criteria of correlation immune pq-valued logical functions are discussed under the CRT-decomposition, so a construction method for correlation immune pq-valued logical functions is derived by the algebraic normal form of the decomposable function.

Keywords: pq-valued logical functions; CRT-decomposition; algebraic standard formula; correlation immunity; decomposition spectrum

Received: 28 Apr 2008. **Accepted:** 06 Nov 2009.

Foundation item: The Open Fund of the State Key Laboratory of Information Security (01-02).